REMARKS

Favorable reconsideration of this application, in light of the preceding amendments and following remarks, is respectfully requested.

Claims 1-22, 25, 27-34, 36, 40, 41 and 43-47 are pending. Claims 1, 9, 29 and 40 are in independent form. Claim 47 is a new claim.

Claim Rejections under 35 U.S.C. § 112, 1st Paragraph

Claims 1, 9 and 29 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement.

In the Amendment dated February 23, 2011, Applicants argued that the language of original claim 1 explicitly supports performing a security check upon each access operation.

In the Response to Arguments section on page 2 of the Office Action, the Examiner alleges that, "[w]hile this may be true, the steps are independent of each other and therefore it cannot be conclude that the permitting of an access operation is dependent on the security check. Further, it is unclear whether a security check is required for permitting an access operation."

Initially, Applicants note that, "the fact that an additional limitation to a claim may lack descriptive support in the disclosure as originally filed does not necessarily mean that the limitation is also not enabled. In other words, the statement of a new limitation in and of itself may enable one skilled in the art to make and use the claim containing that limitation even though that limitation may not be described in the original disclosure." MPEP 2164. Claims 1, 9 and 29 clearly meet the enablement requirement, as is clear by the Examiner's arguments. Therefore, Applicants treat the Examiner's rejection under the written description requirement.

Applicants respectfully note that Applicants' specification as a whole supports a security check both expressly and implicitly. In addition to the arguments of the Amendment dated February 23, 2011, Applicants refer the Examiner to the last two sentences in paragraph [0045] of Applicants' specification as-published (emphasis added):

> In addition, the respective current role of the party accessing data can be established on the basis of the role signature or signatures without this necessitating that further information, e.g., archived service plans or presence lists, be fetched. In this case, the security check 5 ensures **at all times** that the signatures used for documentation are assigned correctly.

As is well known in the art, a presence list indicates the presence of a particular user's device (client) in a network. Accordingly, as one example, it may not be necessary to perform a security check each access operation where a security check has successfully been performed and the personal device of the person accessing data is presently known to be in the area. However, if a presence list indicates that the device is not present, a security check is required at all times, such as where the person accessing data does so from a common use computer or someone else's device.

Withdrawal of the rejections under 35 U.S.C. § 112, 1st paragraph, is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-22, 25, 27-34, 36, 40, 41 and 43-46 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Khidekel (US 2001/0027527, hereinafter "Khidekel") in view of Ballantyne (US 5,867,821, hereinafter "Ballantyne"). Applicants respectfully traverse these rejections.

Role Affiliation

Claim 1 recites, *inter alia*, "each role signature identifying a different activity group with a particular responsibility and at least one role affiliation to the activity group[.]"

The Examiner alleges that, "Khidekel teaches ... assigning at least one role signature, each role signature being assignable to a plurality of users, on the basis of the performed security check without being viewable by the user; [see paragraph 0039] "...business rules that indicate which users are authorized to take various types of actions ..." Office Action, p. 4.

Applicants respectfully submit that even assuming, *arguendo*, that Khidekel discloses identifying a different activity group with a particular responsibility (which applicants do not admit), Khidekel fails to disclose a role signature identifying both an activity group and a role affiliation. Khidekel discloses that, "each page can be marked with business rules that indicate which users are authorized to take various types of actions ... a particular user or ... user groups ... [f]or example hospital administrative staff ... medical staff ... specified physicians[.]" Khidekel, paragraph [0039]. Khidekel does not disclose, at least, role affiliations to activity groups as recited by claim 1. Ballantyne does not disclose either an activity group or a role affiliation and cannot repair the deficiency of Khidekel.

Storage

Claim 1 recites, *inter alia*, "wherein the user signature is recorded in a user signature memory and in the audit memory, the accessed data is stored in an application data store, and the at least one role signature is recorded in a role signature memory and in the audit memory."

The Examiner acknowledges that Khidekel fails to disclose, "wherein each access operation is recorded in an audit memory, the user signature is recorded in the audit memory, and the at least one role signature is recorded in the audit memory[.]" The Examiner, "relies upon the Ballantyne reference ... at col. 8, lines 1-64[,]" to repair the deficiency of Khidekel. Office Action, pp. 4 and 5.

Ballantyne does not disclose any memories or data store in col. 8, lines 1-64. The Examiner appears to allege that Ballantyne discloses an audit memory. The Examiner does not point to any element of Ballantyne for disclosure of a user signature memory and a role signature memory. Even assuming, *arguendo*, that Ballantyne does disclose an audit memory (which Applicants do not admit), Ballantyne fails to disclose, at least, "a user signature memory[,]" "an application data store[,]" and, "a role signature memory[.]"

Nonobviousness

Neither Khidekel nor Ballantyne, alone or in combination, disclose every element of claim 1. Therefore, even assuming, *arguendo*, that Ballantyne could be combined with Khidekel (which applicants do not admit), Khidekel in view of Ballantyne cannot render claim 1 obvious. Claims 9, 29 and 40 are patentable for reasons at least somewhat similar to those stated above for claim 1. Claims 2-8, 10-22, 25, 27, 28, 30-34, 36, 41 and 43-47 are each patentable at least by virtue of their dependency from one of claims 1, 9, 29 and 40. Withdrawal of the rejections and allowance of claims 1-22, 25, 27-34, 36, 40, 41 and 43-47 are respectfully requested.

Claim 7

Claim 7 recites, "wherein the at least one role signature is a plurality of role signatures."

The Examiner alleges that, "Khidekel teaches ... the at least one role signature is a plurality of role signatures.. [see paragraph 0039, wherein specified physicians may be permitted to view patient records as well as modify them while administrative staff may only view patient records]." Office Action, p. 6.

Applicants note that claim 7, which depends from claim 1, requires the assignment of a plurality of role signatures, each role signature being assignable to a plurality of users, on the basis of the performed security check, where the performed security check ascertains the identity of a user, and signing each access operation by specifying the user signature and the plurality of role signatures.

Khidekel nowhere discloses assigning a plurality of role signatures based on a security check. Accordingly, the Examiner appears to allege that claim 7 is inherent in the disclosure of Khidekel. However, the alleged roles in the portion of Khidekel cited to by the Examiner are incompatible. The 'specified physician' category and the 'administrative staff' category are not both assignable based on a security check of a user at least because they are mutually exclusive. Authorization to modify and prohibition from modifying are not compatible permissions. This distinction arises because Khidekel and Ballantyne are directed to access authentication while claim 7 is directed to documenting access in a particular manner. Therefore, even assuming, *arguendo*, that Khidekel does disclose roles (which Applicants do not admit), Khidekel fails to disclose assigning a user signature and a plurality of role signatures on the basis of the performed security check of the user, as required by claim 7. Withdrawal of the rejection and allowance of claim 7 is respectfully requested.

New Claim

Claim 47 is a new claim. Applicants respectfully submit that claim 47 is patentable at least by virtue of its dependency from claim 1. Allowance of claim 47 is respectfully requested.

CONCLUSION

In view of the above remarks and amendments, Applicants respectfully submit that each of the pending objections and rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to contact the undersigned.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By

Donald J. Daley, Reg. No. 34,313
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

DJD/AXV:jrm